THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI SOUTHERN DIVISION

IN THE MATTER OF THE SEARCH OF: **1131 SOUTH PAULA AVENUE SPRINGFIELD, GREENE COUNTY, MISSOURI 65804**	**Case No. 21-SW-2165DPR (UNDER SEAL)**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jeremy Bluto, a Special Agent (SA) with the Homeland Security Investigations, Immigration and Customs Office (HSI / ICE), being first duly sworn, hereby depose and state as follows:

1. I am a Special Agent (SA) with Immigration and Customs Enforcement (ICE) / Homeland Security Investigations (HSI), Kansas City, Missouri, Principal Field Office, and have been so employed since April 25, 2010. I am currently assigned as a criminal investigator for HSI. Prior to my current position, I was employed with U.S. Customs and Border Protection, Office of Border Patrol, as a Border Patrol Agent and a Supervisory Border Patrol agent for five years, and a Deputy Sheriff with the Taney County, Missouri, Sheriff's Department for three years. Prior to my employment in Missouri, I attended California State University, Fullerton, and received a bachelor's degree in Criminal Justice.

2. As part of this affiant's duties with HSI, I investigate criminal violations relating to child exploitation and child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A.

3. The statements in this affidavit are based on my personal observations, training and experience, investigation of this matter, and information obtained from other agents and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, this

affiant has not included each and every fact known to me concerning this investigation. This affiant has set forth the facts necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, are currently located at **1131 South Paula Avenue, Springfield, Greene County, Missouri 65804**, also a location within the Western District of Missouri.

4. This affidavit is in support of an application for a search warrant for evidence, fruits, and instrumentalities of the foregoing criminal violations, which relate to the knowing possession, receipt, distribution, and/or production of child pornography. The property to be searched is described in the following paragraphs and fully in Attachment A. This affiant requests the authority to search and/or examine the seized items, specified in Attachment B, as instrumentalities, fruits, and evidence of crime.

5. This affiant has probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, involving the use of a computer, in or affecting interstate commerce, to produce, receive, possess and / or distribute child pornography, are located in and within the aforementioned property described below. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the aforementioned crimes are located in this property.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of 18 U.S.C. §§ 2251, 2252, and 2252A, relating to material involving the production, receipt, possession, and/or distribution of child pornography:

a. 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing, or coercing a minor to engage in sexually explicit conduct for the

purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce, or if such visual depiction actually was transported in or affecting interstate commerce.

b. 18 U.S.C. § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

c. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

7. The following definitions apply to this Affidavit and its Attachments:

a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term "sexually explicit conduct," 18 U.S.C. § 2256(2)(A)(i-v), includes actual or simulated: (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality;

(c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

c. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

d. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to, or operating in conjunction with, such device.

e. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

a. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

b. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

c. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

f. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, and paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to, phonograph records, printing, and typing) or electrical, electronic, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

h. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

i. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

j. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transfer Protocol (HTTP).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. Based on this affiant's knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom this affiant has had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

9. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

10. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

12. The Internet affords individuals several different venues for meeting one another, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

13. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Google, and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer and/or other electronic devices in most cases.

14. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic

tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

CELLULAR PHONES AND CHILD PORNOGRAPHY

15. Based on this affiant's knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom this affiant has had discussions, cellular phones have likewise revolutionized the manner in which child pornography is produced and distributed.

16. Cellular phones ("cell phones") are exceptionally widespread. The Central Intelligence Agency estimates that in 2016 there were 416 million cell phone subscribers in the United States. Cell phones increasingly offer features such as integrated digital cameras, the ability to store hundreds of digital images, and the ability to access and browse the Internet.

17. In this affiant's training and experience, the ready availability and personal nature of cell phones has led to their frequent use in the commission of child pornography offenses. Individuals with a sexual interest in children will often use their cell phone to browse the Internet and to distribute, receive, and store child pornography files. Individuals producing child pornography will also frequently use the integrated digital camera within a cell phone to produce the images, and then store the images both on the phone and on other devices – such as computers and computer storage media.

18. Cell phones, like other computer systems, will frequently retain data relating to activities, such as Internet browsing history, digital images, and other digital data, that can remain stored for a long period of time.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND CELL PHONES

19. Searches and seizures of evidence from computers and cell phones commonly require agents to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer-related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish fully on-site.

b. Searching computer systems and cell phones for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

20. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media).

21. Furthermore, because there is probable cause to believe that the computer, its storage devices and cell phones are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

BACKGROUND OF INVESTIGATION

22. On October 13, 2021, HSI SA Jeremy Bluto received three CyberTips (CT) submitted by Google LLC to the National Center for Missing and Exploited Children (NCMEC).

CT 100794679 and CT 100821754 were received by NCMEC on September 10, 2021. CT 102087024 was received by NCMEC on September 21, 2021.

23. CT 100794679, 100821754, and 102087024, were all related to the same Google account with the following information:

a. Name: Scott Dunn

b. Mobile Phone: +14172993977 (Verified 01-27-2021 09:19:00 UTC)

c. Email Address: faolin83@gmail.com

d. Email Address: bobsco83@alltel.blackberry.com

24. CT 100794679 documents the upload of 19 files. All of the files submitted were either viewed by Google or compared against a database of previously identified images of child exploitation and found to have a matching hash value. Of the 19 files, six are videos and 13 are still images. SA Bluto reviewed the files, and all the files appear to depict children under the age of 18. Based on SA Bluto's training and experience, all of these files depicted child pornography, that is minors engaged in sexually explicit conduct. The following are details of several files associated with this CT with a description of the contents provided by SA Bluto.

a. File name "report_6069112316783321763," with MD5 hash value 2b24289c47b637c2efcc17279095942, was uploaded on June 23, 2020, at 15:17:41 UTC from IP address 173.19.114.5. This file was a still image and depicted a prepubescent female, who appeared to be less than eight years of age. The prepubescent female was naked below the waist, lying on her back with her legs open, and her vagina and anus exposed. The hand of an adult was visible and was digitally penetrating the anus of the prepubescent female with the index finger.

b. File name "Google-CT-RPT-dab2faff73ef2c18170fec14398d9a10-2021-09-08," with MD5 hash value 3135614d5e76d1ab864ec5b6799c1bb5, was uploaded on September 9, 2021, at 06:19:13 UTC from IP address 2600:387:c:2e12::157. This was a video file, 0:01:17 in length, and depicted a prepubescent female, who appeared to be approximately five to seven years of age, lying naked on a bed. The prepubescent female had her vagina and anus exposed due to her legs being spread open and pushed back toward her shoulders by an adult female. The adult female is naked and has an artificial penis, several inches in length, strapped around her waist in front of her vagina. The adult female inserts the artificial penis into the anus of the prepubescent female. As the adult female proceeds to push the artificial penis in and out, the prepubescent female starts to cry and push against the adult female with her feet. The adult female moves her hands from the prepubescent female's thighs to her shin's and pushes back and continues to thrust aggressively. The adult female then flips the prepubescent female over onto her hands and knees and continues to penetrate her anus with the artificial penis from behind.

c. File name "report_1757068245326501172l.jpg," with MD5 hash value 3135614d5e76d1ab864ec5b6799c1bb5, was uploaded on September 9, 2021, at 06:19:13 UTC from IP address 2600:387:c:2e12::157. The file was a still image and depicted a prepubescent female, who appeared to be less than four years of age. The prepubescent female was on her knees with her vagina and anus exposed and her head turned sideways and laying on the ground. The prepubescent female was naked, and her diaper can be seen on the ground between her knees. The penis of what appeared to be an adult male is positioned behind the prepubescent female with the penis just outside of her vagina/anus.

d. File name "Google-CT-RPT-3250f412145cc14c2060712c952e9357-2021-09-08," with MD5 hash value 68252118565bbc5372a03227138e6656, was uploaded on September 9, 2021, at 06:29:21 UTC from IP address 2600:387:c:2e12::157. This was a video file, 0:01:53 in length, and depicted a prepubescent female, who appeared to be less than ten years of age, lying naked on a bed. The prepubescent female had her legs spread open with her vagina and anus exposed. The head, face, and hands of an older female, who appeared to be in her late teens, was visible. The older female was performing oral sex, rubbing, and digitally penetrating the vagina of the prepubescent female.

25. CT 100821754 documented the upload of two files. Neither of the files submitted were viewed by Google but were compared against a database of previously identified images of child exploitation and found to have a matching hash value. Both files were videos. SA Bluto reviewed the files, and both files appeared to depict children under the age of 18. Based on SA Bluto's training and experience, these filed depicted child pornography, that is minors engaged in sexually explicit conduct. The following are details of the files associated with this CT and a description of the contents provided by SA Bluto.

a. File name "Google-CT-RPT-053b82c6fe67c8675a8c5aed579c3a2e-2021-09-08," with MD5 hash value 5a7135fdeda927862caae9a72b458a1b, was uploaded on September 9, 2021, at 06:20:06 UTC from IP address 2600:387:c:2e12::157. This was a video file, 0:01:30 in length, and depicted a prepubescent female, who appeared to be less than ten years of age, naked and lying face down on top of another female, also naked, who appeared to be in her late teens. The prepubescent female had her head between the legs of the older female and her vagina and anus near the head of the older female. The older

female was performing oral sex on the prepubescent female and digitally penetrating her vagina.

b. File name "Google-CT-RPT-1bc18817138d9d0e0b66221824fab8fe-2021-09-08," with MD5 hash value d1f80990e2490be3f59e631f4cda38bc, was uploaded on September 9, 2021, at 06:25:03 UTC, from IP address 2600:387:c:2e12::157. This was a video file, 0:00:25 in length, and depicted a prepubescent female, who appeared to be less than ten years of age, lying on her back with her vagina exposed and her legs spread open. A hand that appears to be from an adult was rubbing and digitally penetrating the vagina of the prepubescent female throughout.

26. CT 102087024 documents the upload of one file. The file was viewed by Google and determined to contain an image of child exploitation. The file was a still image. SA Bluto reviewed the file, and it appeared to depict a child under the age of 18. The following are details of the file associated with this CT and a description of the contents provided by SA Bluto.

a. File name "report_1596495720255291397," with MD5 hash value 8631953e5b928d64dca47b96c70bda08, was uploaded on April 10, 2018, at 02:23:43 UTC, from IP address 2604:2d80:c407:8984:5d97:88e2:3aae:34b9. This was a still image and depicted a prepubescent female who appears to be under 12 years of age. The prepubescent female was sitting on her buttocks with her knees bent and her legs spread. She was wearing a grey t-shirt and tan colored underwear. The underwear is pushed to the side, exposing her vagina, which was the central focus of the image.

27. IP address 173.19.114.5 was determined to be assigned to Mediacom Communications (Mediacom). As part of the investigation, an investigative subpoena requesting

subscriber information for IP address 173.19.114.5 on June 23, 2020, was served on Mediacom on October 27, 2021.

28. On November 1, 2021, Mediacom identified the subscriber to IP address 173.19.114.5 on June 23, 2020, as Babbette Farrow, with a service address of **1131 South Paula Avenue, Springfield, Missouri 65804**.

29. IP address 2600:387:c:2e12::157 was determined to be assigned to AT&T Wireless. Based on prior investigations it is known that AT&T Wireless is unable to provide subscriber information for IP addresses when the request comes more that 48 hours after the connection is established. This investigation began more than 48 hours after the connection to IP Address 2600:387:c:2e12::157 was established, so an investigative subpoena was not issued.

30. The information provided to NCMEC from Google, and contained within the CT, included a phone number associated with the suspect Google account. Phone number +14172993977 was associated with the suspect Google account and the phone number was verified by Google on January 27, 2021.

31. Phone number +14172993977 was found to be assigned to AT&T Wireless. As part of the investigation, an investigative subpoena requesting subscriber information for phone number +14172993977, was served on AT&T Inc. on October 27, 2021.

32. On October 29, 2021, AT&T Inc. identified the account holder of phone number +14172993977 as Babbette E. Farrow, with a billing address of **1131 South Paula Avenue, Springfield, Missouri 65804**. AT&T also indicated phone number +14172993977 was ported to AT&T on January 30, 2021.

33. The information provided to NCMEC from Google, and contained within the CT, included a connection log which captured the IP address used when connections were made to the

suspect Google account. The connection log lists several other IP addresses assigned to AT&T Wireless and also lists IP address 108.230.186.12 as establishing a connection to the suspect Google account 25 times dating back to January 30, 2021.

34. IP address 108.230.186.12 was determined to be assigned to AT&T U-Verse. As part of the investigation, an investigative subpoena requesting subscriber information for IP address 108.230.186.12 beginning on January 30, 2021, was served on AT&T Inc. on October 27, 2021.

35. On October 30, 2021, AT&T Inc. identified the subscriber of IP address 108.230.186.12 beginning on January 30, 2021, as Babbette Farrow, with a service address of **1131 South Paula Avenue, Springfield, Missouri 65804**.

36. IP address 2604:2d80:c407:8984:5d97:88e2:3aae:34b9 was determined to be assigned to Mediacom Communications (Mediacom). As part of the investigation, an investigative subpoena requesting subscriber information for IP address 2604:2d80:c407:8984:5d97:88e2:3aae:34b9 on April 10, 2018, was served on Mediacom on November 15, 2021.

37. On November 15, 2021, Mediacom responded and indicated they did not have any records pertaining to IP address 2604:2d80:c407:8984:5d97:88e2:3aae:34b9 on April 10, 2018.

38. Records show that phone number +14172993977 was assigned to Verizon Wireless prior to being ported to AT&T on January 30, 2021. As part of the investigation, an investigative subpoena requesting subscriber information related to phone number +14172993977 prior to January 30, 2021, was served on Verizon Wireless on November 16, 2021.

39. On November 29, 2021, Verizon Wireless responded and indicated the account holder of phone number +14172993977 prior to January 30, 2021, was Babbette Farrow with a billing address of **1131 South Paula Avenue, Springfield, Missou**ri.

40. The connection log provided to NCMEC by Google and described in paragraph 33 above, also showed five connections to the suspect Google account from three separate IP addresses assigned to Verizon Business. IP address 2600:100a:b110:954b:19a5:5fa3:9fd:ffbf connected on December 8, 2020, at 01:15:33 UTC and December 8, 2020, at 01:15:41 UTC. IP address 2600:100a:b11a:c84f:9d5e:52cd:6012:38c connected on December 22, 2020 at 01:03:21 UTC and December 22, 2020 at 01:03:22 UTC. IP address 2600:100a:b110:fcb5:2cd5:c7e0:41f4:af65 connected on January 21, 2021 at 05:50:56 UTC. As part of the investigation, an investigative subpoena requesting subscriber information related to the IP addresses listed on the stated dates and times, was served on Verizon Business on November 16, 2021.

41. On November 29, 2021, Verizon Business responded and indicated the IP addresses were actually owned by Verizon Wireless and forwarded the subpoena to them. On the same date, Verizon Wireless responded and indicated IP address 2600:100a:b110:954b:19a5:5fa3:9fd:ffbf connected on December 8, 2020, at 01:15:33 UTC and December 8, 2020, at 01:15:41 UTC, IP address 2600:100a:b11a:c84f:9d5e:52cd:6012:38c connected on December 22, 2020, at 01:03:21 UTC and December 22, 2020, at 01:03:22 UTC, and IP address 2600:100a:b110:fcb5:2cd5:c7e0:41f4:af65 connected on January 21, 2021, at 05:50:56 UTC, were all wireless connections established by Verizon Wireless phone number +14172993977.

42. On November 16, 2021, Springfield City Utilities records were queried and revealed the utilities at **1131 South Paula Avenue** are in the name of Babbette Farrow.

43. Beginning on November 16, 2021, and on several subsequent dates, SA Bluto conducted an address check of **1131 South Paula Avenue, Springfield, Missouri**. SA Bluto observed a red in color, Acura MDX bearing Missouri license plate RA7 G1U. Missouri motor vehicle records revealed that Missouri RA7 G1U is registered to Scott A. DUNN, transfer on death to Sheila Dunn, with an address of **1131 South Paula Avenue, Springfield, Missouri**.

44. In the information provided by NCMEC by Google, the accounts holder was listed as Scott DUNN. The two email addresses associated with the account were faolin83@gmail.com and bobsco83@alltell.blackberry.com. Scott Alan DUNN was born on December 12, 1983. Based on my training and experience, it is common for people to include a number associated with their birth year in their email addresses.

45. Open source and law enforcement databases were queried and revealed that Babette Farrow, Scott DUNN, and Sheila Dunn, were all associated with the address **1131 South Paula Avenue, Springfield, Missouri**. Missouri driver records were queried and revealed Scott Alan DUNN's residence address was listed as **1131 South Paula Avenue, Springfield, Missouri**.

46. An open source social media query was conducted and revealed that Babette Huckaba Farrow, Scott DUNN, and Sheila Dunn (Sheila Huckaba) were all friends on Facebook.

PROBABLE CAUSE

47. Based on the above facts, this affiant believes probable cause exists for the issuance of a warrant to search the premises described more fully in Attachment A for (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of a crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means of committing a criminal offense, namely possible

violations of 18 U.S.C. §§ 2251, 2252, and 2252A, including, but not limited to, the items listed in Attachment B.

Further Affiant Sayeth Naught.

JEREMY BLUTO
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me via telephone on the 7th day of December 2021.

HONORABLE DAVID P. RUSH
Chief United States Magistrate Judge
Western District of Missouri